

NOTES ON THE PRINCIPAL PRIMES OF REAL QUADRATIC NUMBER FIELDS

PARK, JEONGHO

ABSTRACT. Several notes on the fundamental units of real quadratic fields are presented, and the problem about the class number is translated to one about the decomposition of a single rational prime into principal ideals. We give an explicit construction of all real quadratic number fields in which given prime p splits or ramifies into principal primes.

INTRODUCTION

The ideal class group of a number field K admits a huge theory. The algebraic side of it appears as the central subject in class field theory which translates the problem into one about field extensions, namely into the questions of how far we have to climb up to principalize every ideal. On this point of view the interest is on a fixed number field, and the class number is the reciprocal of the Dirichlet density of principal prime ideals. An intrinsic connection between the class group and the image of the norm map is also a classic, and Hasse norm theorem changes the subject into one on a local setting.

The analytic and quantitative side of class groups is expressed in terms of asymptotic behaviors, which are mainly about the magnitude of class groups. The interest is on the chances for a family of number fields to have a proper size of class number; for real quadratic case, which this paper is about, the most important problem in this direction is to show that in most cases the class group is very small compared to the field discriminant. The so-called Cohen-Lenstra Heuristics and other conjectures appeared in [15], [20], the conjectures proposed in [5], or the classical Gauss' conjecture all

Date: August 27, 2012.

1991 *Mathematics Subject Classification.* Primary:11R29, Secondary: 11R37, 11Y40, 11J68.

Key words and phrases. Real quadratic number field, Class number, Fundamental unit, Principal ideal, Prime ideal.

Supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (2010-0026473).

are about this aspect of class group, and very little can be said about these problems at this moment.

When K is a real quadratic number field $\mathbb{Q}(\sqrt{d})$, knowing the size h_d of its class group is almost equivalent to knowing the size of the fundamental unit, as immediately indicated by the famous class number formula of Dirichlet and the logarithmic bound of the L -values. The fundamental unit ε_d comes from the continued fraction expansion of \sqrt{d} or $\frac{\sqrt{d}+1}{2}$ whose period l is the most dominant factor in the size of ε_d . As one can expect, many researches have been focused on the period and now its upper bound is known to a precision; See [6] and [10]. The lower bound of the average order of ε_d is, however, known only to the following extent; for almost all non-square d , one has $\varepsilon_d > d^{\frac{7}{4}-\epsilon}$ ([7], [8]).

A simple fact is that the magnitude of the fundamental unit increases as there are more rational primes $p \ll \sqrt{d}$ that split into principal primes $P\overline{P}$ in $\mathbb{Q}(\sqrt{d})$ (see [23]; an effective sharp bound can also be found with the method in [16]). Another fact is that (see section 5) if $p < \sqrt{d}/2$ and ξ and $\tilde{\xi}$ are the least elements in P and \overline{P} greater than 1, then $\xi\tilde{\xi} = p\varepsilon_d$. This suggests that *a full knowledge about a single principle prime and its conjugate gives a full information about ε_d* . It is not difficult to show that almost always a quadratic integer whose norm is a given prime is the least element of the ideal it is contained; see [16]. The central obstacle, as natural, is to show that ξ and $\tilde{\xi}$ are very far apart from each other in most cases.

The aim of this paper is to deal with the algebraic side of ideal class group in analytic point of view, by considering the principal prime ideals based on the continued fraction expansion of \sqrt{d} or $\frac{\sqrt{d}+1}{2}$. The thing is that if L is the Hilbert class field of $K = \mathbb{Q}(\sqrt{d})$, not only the image of the norm map $N_{L/K}$ and prime decomposition in L/K are key blocks in the structure of the class group of K , but also are the image of $N_{K/\mathbb{Q}}$ and prime decomposition into principal primes in K/\mathbb{Q} ; the former is in algebra, the latter is in analysis. This paper is about the latter one.

It begins with an argument about the fundamental solutions to Pell's equation, which is quickly generalized to one about the norms of quadratic integers. Short intervals assigned to rational numbers give rise to a set of quadratic progressions that covers non-square d 's for which a specified rational prime splits into principal prime ideals. The condition of being square-free is difficult to integrate for individual integer d , so we will consider the density of square-free numbers in a sequence and specify exactly what portion of integers in consideration is square-free. A byproduct of the 'analytic' story is that $h_d > 1$ for any square-free integer d such that two or more primes $p \ll d^{1/4}$ ramify in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, which is a weaker statement than that implied by Gauss' genus theory.

The statements are not focused on prime numbers though, as the approach carries its full strength over general integers too. The implications about principal prime ideals can be read in the literature immediately. Throughout this paper we stick to the ring $\mathbb{Z}[\sqrt{d}]$ for the ease of statements, and conclusions for the case $d \equiv 1 \pmod{4}$ are dealt with in section 6 separately.

1. PRELIMINARIES

Let D be the field discriminant of $\mathbb{Q}(\sqrt{d})$.

We first mention a quantitative conjecture by Hooley, which serves as a landmark in class number problem on analytic base.

Conjecture 1.0.1 ([5]).

$$\sum_{0 < D < 4x, 4 \mid D} h_d \sim \frac{25}{12\pi^2} x (\log x)^2$$

Throughout this paper μ represents a rational integer that is comparatively small, and d a non-square positive integer which is considered to be large. Let $\sqrt{d} = [a_0, a_1, a_2, \dots]$ be the simple continued fraction expansion, $l = l(\sqrt{d})$ the period of \sqrt{d} , $\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$ a convergent, $\alpha_{n+1} = [a_{n+1}, a_{n+2}, \dots]$ the $(n+1)$ -th total quotient, and $N(x)$ the usual norm of $x \in \mathbb{Q}(\sqrt{d})$. Put $\xi_n = p_n + q_n \sqrt{d}$ and $\nu_n = |N(\xi_n)|$. We say that a quadratic integer ξ comes from a convergent to \sqrt{d} when ξ is of this form.

We simply recall that the continued fraction of $\sqrt{d} + \lfloor \sqrt{d} \rfloor$ is symmetric, purely periodic and the fundamental solution to the Pell's equation $X^2 - dY^2 = \pm 1$ comes from the first period of \sqrt{d} , namely $\varepsilon_d = \xi_{l-1}$. In case $d \equiv 1 \pmod{4}$ a convergent p_n/q_n to $\frac{1+\sqrt{d}}{2}$ gives the fundamental unit of $\mathbb{Q}(\sqrt{d})$ in the form $\xi_n = p_n - q_n + q_n \frac{1+\sqrt{d}}{2}$; see [16] for the details.

The followings will be used freely in the sequel.

Proposition 1.0.2 ([13]). *If $(p, q) = 1$ and*

$$\left| \frac{p}{q} - x \right| < \frac{1}{2q^2}$$

then p/q is a convergent to x .

Lemma 1.0.3 ([16]). (1) *For $n \geq 0$*

$$\alpha_{n+1} = \frac{\sqrt{D}}{\nu_n} - \frac{q_{n-1}}{q_n} + O\left(\frac{1}{q_n^2 \sqrt{D}}\right).$$

- (2) *every quadratic integer whose norm is less than $\sqrt{D}/2$ and is square-free comes from a convergent to \sqrt{d} or $\frac{1+\sqrt{d}}{2}$.*

Note that

$$N(p + q\sqrt{d}) = p^2 - q^2d = \mu \Rightarrow \left| \frac{p}{q} - \sqrt{d} \right| = \frac{|\mu|}{(p + q\sqrt{d})q}$$

Therefore the norm of a quadratic integer measures how efficient the approximation of \sqrt{d} by $\frac{p}{q}$ is. In particular, a quadratic unit appears when this efficiency is the best.

Lemma 1.0.3 also tells us that the partial quotients that can arise in the expansion of \sqrt{d} are very restricted, namely $\frac{2\sqrt{d}}{n} + O(1)$ for $n \in \mathbb{Z}$. The situation is more precise when d is sufficiently large; if ν_n and ν_m are relatively small so that $\frac{\sqrt{D}}{\nu_i} - \frac{\sqrt{D}}{1+\nu_i} = \frac{\sqrt{D}}{\nu_i(1+\nu_i)} > 2 + \epsilon$, then $a_{n+1} = a_{m+1}$ if and only if $\nu_n = \nu_m$.

2. THE SQUARE-FREE INTEGERS

Let $Q(x)$ be the number of square-free integers between 1 and x . It is well known that $Q(x) = \frac{6}{\pi^2}x + O(\sqrt{x})$ (for example, see theorem 333 of [13]). In [2], under Riemann hypothesis it was proved that $Q(x) = \frac{6}{\pi^2}x + O(x^{17/54+\epsilon})$. This suggests that about 60.79% of the integers between n^2 and $(n+1)^2$ shall be square-free for every sufficiently large n .

A nice result about congruences also can be found.

Theorem 2.0.4 ([4], [17]). *Let $S(x; a, k)$ be the number of square-free integers that do not exceed x and that are congruent to a modulo k . Assume $(a, k) = 1$ and $k \leq x^{2/3-\epsilon}$. Then*

$$S(x; a, k) \sim \frac{6x}{\pi^2 k} \prod_{p|k} \left(1 - \frac{1}{p^2}\right)^{-1} \quad (x \rightarrow \infty)$$

In particular, $S(x; 1, 4) \sim S(x; 3, 4) \sim \frac{1}{3} \frac{6}{\pi^2} x$ and each third of square-free numbers is congruent to 1, 2, 3 modulo 4.

The following theorem will prove useful too. (In following sections we only need its strength for quadratic polynomial, which can be proved unconditionally using the sieve of Eratosthenes; See [14].)

Theorem 2.0.5 ([14], [3]). *Suppose that $f(x) \in \mathbb{Z}[x]$ has no repeated root. Let B be the largest integer which divides $f(n)$ for all integer n , and select B' to be the smallest divisor of B for which B/B' is square-free. If the abc-conjecture is true, then there are $\sim C_f N$ positive integers $n \leq N$ for*

which $f(n)/B'$ is square-free, where $C_f > 0$ is a positive constant, which we determine as follows;

$$C_f = \prod_{p: \text{ prime}} \left(1 - \frac{\omega_f(p)}{p^{2+q_p}} \right)$$

where, for each prime p , we let q_p be the largest power of p which divides B' and let $\omega_f(p)$ denote the number of integers a in the range $1 \leq a \leq p^{2+q_p}$ for which $f(a)/B' \equiv 0 \pmod{p^2}$.

3. THE FUNDAMENTAL UNIT

Numerical evidence suggests that the regulator $R_d = \log \varepsilon_d$ reaches the size of \sqrt{d} closely for most of d , and in that case lemma 1.0.3 implies that the partial quotients in the expansion of \sqrt{d} are bounded and their variation contributes only $O(\log d)$. Therefore the period l dominates the size of R_d . There is a small ambiguity depending on the residue of d modulo 4 though; one have to choose the continued fraction of \sqrt{d} or that of $\frac{1+\sqrt{d}}{2}$ accordingly. Such ambiguity causes little difference in the size of R_d as indicated in [18] and [21] by following theorem. (The original statement of this inequality is sharper on a case-by-case setting; see the references)

Theorem 3.0.6 ([21]). *For any non-square $d \equiv 1 \pmod{4}$*

$$\frac{1}{3}l \left(\frac{1 + \sqrt{d}}{2} \right) \leq l(\sqrt{d}) \leq 5l \left(\frac{1 + \sqrt{d}}{2} \right)$$

Therefore it suffices to work with \sqrt{d} in an asymptotic point of view. In the sequel we use ε_d to denote the fundamental solution to the Pell's equation $X^2 - dY^2 = \pm 1$ (i.e., the least unit in $\mathbb{Z}[\sqrt{d}]$ among those greater than 1). Note that in an ideal-based argument, the use of ε_d instead of the fundamental unit has no shortcomings even when $d \equiv 1 \pmod{4}$. For such d , some powers of the fundamental unit of $\mathbb{Q}(\sqrt{d})$ are in $\mathbb{Z}[\sqrt{d}]$ and theorem 3.0.6 tells us that the least exponent in these powers is bounded. Precisely, it can be proved that the fundamental unit or its cube is in $\mathbb{Z}[\sqrt{d}]$; see [22] and its references. The story in the previous section also tells us that a result about large density of non-square d can be translated to a result about square-free d .

Recalling the class number formula and bounds of the L -values, an upper bound of $l(\sqrt{d})$ can be found. Indeed the following has been known for decades.

Proposition 3.0.7 ([6]). (a) $l(\sqrt{d}) \ll \sqrt{d} \log d$.

(b) $l(\sqrt{d}) \neq o\left(\frac{\sqrt{d}}{\log \log d}\right)$.

In [19] it was also mentioned that the average of $l(\sqrt{d})$ for $n^2 < d < (n+1)^2$ is less than $\frac{7n+3}{4}$.

As for the lower bound of $l(\sqrt{d})$, conjecture 1.0.1 suggests that $l(\sqrt{d}) \gg \frac{\sqrt{d}}{(\log d)^2}$ on average. Still Gauss's conjecture remains out of reach and it is notoriously difficult to prove the abundance of fundamental discriminants whose class group is very small.

A real quadratic field with small fundamental unit is an exceptional one. When the period is small, an explicit description of every non-square d 's with such periods can be made. A few of them are listed below:

$$\begin{aligned} l(\sqrt{d}) = 1 &\iff \sqrt{d} = a_0 + \frac{1}{a_0 + \sqrt{d}} \\ &\iff a_0\sqrt{d} + a_0^2 + 1 = d + a_0\sqrt{d} \\ &\iff d = a_0^2 + 1 \end{aligned}$$

$$\begin{aligned} l(\sqrt{d}) = 2 &\iff \sqrt{d} = a_0 + \frac{1}{a_1 + \frac{1}{a_0 + \sqrt{d}}} \\ &\iff \sqrt{d} = \frac{2a_0 + a_0^2a_1 + (a_0a_1 + 1)\sqrt{d}}{1 + a_0a_1 + a_1\sqrt{d}} \\ &\iff d = a_0^2 + \frac{2a_0}{a_1} \\ &\iff d = a_0^2 + b, \quad b \mid 2a_0, \quad b \geq 2 \end{aligned}$$

and similarly one can show that

$$\begin{aligned} l(\sqrt{d}) = 3 &\iff \dots \\ &\iff d = (4a^2b + a + b)^2 + 4ab + 1, \quad a, b \geq 1 \end{aligned}$$

$$\begin{aligned} l(\sqrt{d}) = 4 &\iff \dots \\ &\iff \begin{cases} d = (4ab - 2b + 2)c + r_1 + R_1, & b \text{ is odd} \\ d = (ab + 1)c + r_2 + R_2, & b \text{ is even} \end{cases} \end{aligned}$$

where $a, b \geq 1$, $c \geq 0$, $0 < r_1 < 4ab - 2b + 2$, $0 < r_2 < ab + 1$,

$$r_1 \equiv ((2a - 1)(2ab - b + 2))^{-1} b \pmod{4ab - 2b + 2}$$

$$r_2 \equiv \left(a + a^2 \frac{b}{2}\right)^{-1} \frac{b}{2} \pmod{ab + 1}$$

and

$$R_1 = \left(c(2a-1)(2ab-b+2) + \frac{r_1(2a-1)(2ab-b+2)-b}{4ab-2b+2} \right)^2$$

$$R_2 = \left(ac(1 + \frac{ab}{2}) + \frac{r_2a(ab+2)-b}{2ab+2} \right)^2$$

As the length grows the expression quickly becomes a mess. Indeed, length $l = n$ means there can be n variables to be chosen freely, whence we see that such formulation would not be a natural one for longer periods.

4. THE ATTACHED INTERVALS AND MINIMAL TYPES

Recall that every irrational number has a unique continued fraction expansion. It is a simple observation that the real line is partitioned by the predecessors, i.e., for any a_0, a_1, \dots, a_m the set

$$\{x \in \mathbb{R} \mid x = [a_0, a_1, a_2, \dots, a_m, *]\}$$

is a closed interval. Let q_t be the denominator of $[0, a_1, a_2, \dots, a_t]$. The following proposition quantifies these intervals.

Proposition 4.0.8. *Let a_1, a_2, \dots, a_m be positive integers and $f(N)$ the number of non-square d 's between 1 and N such that*

$$\sqrt{d} = [a_0, a_1, a_2, \dots, a_m, *]$$

Then

$$\lim_{N \rightarrow \infty} \frac{f(N)}{N} = \frac{1}{q_m(q_m + q_{m-1})}.$$

We give a sketch of proof. Consider the numbers in the interval $(n^2, (n+1)^2)$. The graph $y = \sqrt{x}$ is almost linear in $n^2 < x < n^2 + 2n + 1$, and the difference between $[n, a_1, a_2, \dots, a_m] = [n, a_1, a_2, \dots, a_m, \infty]$ and $[n, a_1, a_2, \dots, a_m + 1]$ is $\frac{1}{q_m(q_m + q_{m-1})}$. The computation with a proper estimation of the errors is straightforward.

Based on lemma 1.0.3 and the comments below it, for each finite sequence $\frac{p}{q} = [a_0, a_1, a_2, \dots, a_m]$ of positive integers we can assign a tiny interval $I_{p/q}$ that consists of points whose square roots are very close to p/q . More specifically, we want this interval to satisfy following property: whenever a non-square integer d falls into that interval, the efficiency of approximation of \sqrt{d} by p/q is the best and $p + q\sqrt{d}$ becomes a quadratic unit. Explicitly, we can take the interval as

$$I_{p/q} = \left([a_0, a_1, \dots, a_m, \frac{4}{3}\sqrt{d}]^2, [a_0, a_1, \dots, a_m, 1, \frac{4}{3}\sqrt{d}]^2 \right)$$

(or the reverse of this, according to the parity of m .)

Write $\lfloor \frac{p}{q} \rfloor = a_0 = n = \lfloor \sqrt{d} \rfloor$, so $I_{p/q}$ is an interval in $(n^2, (n+1)^2)$ and we are dealing with non-square d that are in the same range. The factor $\frac{4}{3}$ in the last entry is chosen somewhat arbitrarily; Since the partial quotient cannot take values between $\sqrt{d} + \epsilon$ and $2\sqrt{d} - \epsilon$, any number between $1 + \epsilon$ and $2 - \epsilon$ will be fine.

We denote the fractional part of p/q by $\{p/q\} = k/q$.

Theorem 4.0.9. $I_{p/q}$ contains an integer if and only if

$$k^2 \equiv -1 \pmod{q}, \quad 2n \equiv k \left(\frac{1+k^2}{q} \right) \pmod{q}$$

or

$$k^2 \equiv 1 \pmod{q}, \quad 2n \equiv k \left(\frac{1-k^2}{q} \right) \pmod{q}$$

and in that case the integer d contained in $I_{p/q}$ is given by

$$d = n^2 + 2\frac{k}{q}n + \frac{k^2 \pm 1}{q^2}.$$

Proof. Assume m is even. Then

The interval $\left(\frac{p^2}{q^2}, [n, a_1, \dots, a_m, \frac{4}{3}\sqrt{d}]^2 \right)$ contains an integer

$$\Leftrightarrow \left\lfloor \frac{p^2}{q^2} \right\rfloor - \frac{p^2}{q^2} < \frac{1.5}{q^2}$$

$$\Leftrightarrow \left\{ \frac{p}{q} \right\}^2 + 2n \left\{ \frac{p}{q} \right\} \pmod{1} \in \left(1 - \frac{1.5}{q^2}, 1 \right) \pmod{1}$$

$$\Leftrightarrow 2n \left\{ \frac{p}{q} \right\} \pmod{1} \in \left(-\frac{k^2}{q^2} - \frac{1.5}{q^2}, -\frac{k^2}{q^2} \right) \pmod{1}$$

$$\Leftrightarrow 2nk \pmod{q} \in \left(-\frac{k^2}{q} - \frac{1.5}{q}, -\frac{k^2}{q} \right) \pmod{q}$$

$$\Leftrightarrow k^2 \equiv -1 \pmod{q}, \quad 2n \equiv k^{-1} \left(\frac{-1-k^2}{q} \right) \equiv k \left(\frac{1+k^2}{q} \right) \pmod{q}$$

For odd m , a similar computation shows that

The interval $\left([n, a_1, \dots, a_m, \frac{4}{3}\sqrt{d}]^2, \frac{p^2}{q^2} \right)$ contains an integer

$$\Leftrightarrow k^2 \equiv 1 \pmod{q}, \quad 2n \equiv k^{-1} \left(\frac{1-k^2}{q} \right) \equiv k \left(\frac{1-k^2}{q} \right) \pmod{q}$$

Recall that a rational number p/q can have both even or odd length. When this ambiguity is compensated by putting or eliminating 1 at the

last entry, the two half-intervals in the computation unifies to $I_{p/q}$. (The computation can be simplified pretty much and will be given later, but this one shows an idea of where this approach came from.) The expression of d in terms of n, k, q is of triviality, considering the integer closest to $(n + k/q)^2 = n^2 + 2nk/q + k^2/q^2$. \square

Remark 4.0.10. Choose any pair (y, x) with $0 \leq x < y$, $x^2 \equiv 1$ or $-1 \pmod{y}$. Let

$$\tilde{y} = \begin{cases} \frac{y}{2} & \text{if } y \text{ is even} \\ y & \text{otherwise} \end{cases}$$

The set of n 's for which $I_{n+x/y}$ contains an integer d , or equivalently, positive n 's for which an integer d exists between n^2 and $(n+1)^2$ such that $ny + x + y\sqrt{d}$ becomes a quadratic unit, forms an arithmetic progression with common difference \tilde{y} .

For such pair (y, x) , let $\mathfrak{D}(y, x)$ be the set of (non-square) integers d contained in the intervals $\{I_{n+x/y}\}_n$ where n runs through the arithmetic progression. Let $x/y = [0, a_1, a_2, \dots, a_m]$. Then for any $d \in \mathfrak{D}(y, x)$ we have

$$\sqrt{d} = [\lfloor \sqrt{d} \rfloor, \overline{a_1, a_2, \dots, a_m}, 2\lfloor \sqrt{d} \rfloor]$$

and unless $2\lfloor \sqrt{d} \rfloor = \max\{a_1, a_2, \dots, a_m\}$ the period is exactly $m+1$ and $\lfloor \sqrt{d} \rfloor y + x + y\sqrt{d}$ is the fundamental solution to the Pell's equation $X^2 - dY^2 = \pm 1$. (It is easy to show that every solution to this Pell's equation is a power of the fundamental solution even when d has square factors.) Since the partial quotients of \sqrt{d} cannot exceed $2\lfloor \sqrt{d} \rfloor$, such exceptional case can occur only at the least element of $\mathfrak{D}(y, x)$. Let $\overline{\mathfrak{D}}(y, x)$ be the set $\mathfrak{D}(y, x)$ where this possible exception is removed, i.e., with the least element discarded if its period is less than $m+1$. Observe that $\{\overline{\mathfrak{D}}(y, x)\}_{y,x}$ forms a partition of the set of non-square integers.

Combining the notion of $\overline{\mathfrak{D}}(y, x)$ and the theorems in [1], [11], and Theorem 3.1 in [12], following proposition is an immediate corollary.

Proposition 4.0.11. *Let $0 \leq x < y$, $\frac{x}{y} = \frac{p_m}{q_m} = [0, a_1, a_2, \dots, a_m]$, $\frac{p_{m-1}}{q_{m-1}} = [0, a_1, a_2, \dots, a_{m-1}]$, where the parity of m is uniquely determined by*

$$(q_m, p_{m-1}) \not\equiv (0, 1) \pmod{2}.$$

Then

$$\begin{cases} x^2 \equiv 1 \pmod{y} & \Leftrightarrow (a_1, a_2, \dots, a_m) \text{ is symmetric, } m \text{ is odd;} \\ x^2 \equiv -1 \pmod{y} & \Leftrightarrow (a_1, a_2, \dots, a_m) \text{ is symmetric, } m \text{ is even.} \end{cases}$$

If d is the least element of $\overline{\mathfrak{D}}(y, x)$ for some (y, x) , then d is said to be of *minimal type*, which agrees with the definition of *minimal type* for \sqrt{d}

imposed in [12] in a somewhat different fashion. A quantification of the integers of minimal type can be found in the following theorem. In an expository manner, it says that almost all non-square positive integers are of minimal type and the proof also shows that $\overline{\mathfrak{D}}(y, x) = \mathfrak{D}(y, x)$ for almost all d .

Theorem 4.0.12. *Let $\overline{\mathfrak{D}}$ be the set of all non-square positive integers of minimal type. Then*

$$\sum_{d \in \overline{\mathfrak{D}}} \frac{1}{d^s} \approx \zeta(s) \quad \text{as } s \rightarrow 1+.$$

(where ‘ \approx ’ means the difference is bounded.)

Proof. Let $d_0(y, x)$ be the least element of $\mathfrak{D}(y, x)$, and

$$V(y) = \{x \mid 0 \leq x < y, x^2 \equiv \pm 1 \pmod{y}\},$$

$$I_1 = \{(y, x) \mid y \geq 1, x \in V(y), \overline{\mathfrak{D}}(y, x) = \mathfrak{D}(y, x)\},$$

$$I_2 = \{(y, x) \mid y \geq 1, x \in V(y), \overline{\mathfrak{D}}(y, x) \neq \mathfrak{D}(y, x)\}.$$

We can easily compute the following sums:

$$\begin{aligned} \zeta(s) - \zeta(2s) &= \sum_{y=1}^{\infty} \sum_{x \in V(y)} \sum_{d \in \widehat{\mathfrak{D}(y, x)}} \frac{1}{d^s} \\ &= \sum_{(y, x) \in I_1} \left(\frac{1}{d_0(y, x)^s} + \sum_{k=1}^{\infty} \frac{1}{\left((\sqrt{d_0(y, x)} + k\tilde{y})^2 + O(1/y^2) \right)^s} \right) \\ &\quad + \sum_{(y, x) \in I_2} \sum_{k=1}^{\infty} \frac{1}{\left((\sqrt{d_0(y, x)} + k\tilde{y})^2 + O(1/y^2) \right)^s} \\ &= \sum_{(y, x) \in I_1} \left(\frac{1}{d_0(y, x)^s} + \frac{1}{\tilde{y}^{2s}} (\zeta(2s) - O(1)) \right) \\ &\quad + \sum_{(y, x) \in I_2} \frac{1}{\tilde{y}^{2s}} (\zeta(2s) - O(1)). \end{aligned}$$

$V(y)$ can be divided into $V^+(y)$ and $V^-(y)$ where

$$V^+(y) = \{x \mid 0 \leq x < y, x^2 \equiv 1 \pmod{y}\},$$

$$V^-(y) = \{x \mid 0 \leq x < y, x^2 \equiv -1 \pmod{y}\}.$$

Using Chinese remainder theorem and the fact that the group of units modulo p^n for an odd prime p is cyclic, it is easy to see that $x^2 \equiv 1 \pmod{y}$ has $O(2^{\omega(y)})$ roots. The same is true for $x^2 \equiv -1 \pmod{y}$ if -1 is a

quadratic residue for every prime divisor of y ; otherwise it has no solutions. It follows that

$$\sum_{y=1}^{\infty} \sum_{x \in V(y)} \frac{1}{y^{2s}} \ll \sum_{y=1}^{\infty} \sum_{x \in V^+(y)} \frac{1}{y^{2s}} \ll \sum_{y=1}^{\infty} \frac{2^{\omega(y)}}{y^{2s}} = \frac{\zeta(2s)^2}{\zeta(4s)} = O(1)$$

and therefore

$$\sum_{(y,x) \in I_1} \frac{1}{d_0(y,x)^s} \approx \zeta(s) \quad \text{as } s \rightarrow 1+$$

which proves the assertion. \square

5. PRINCIPAL IDEALS AND QUADRATIC PROGRESSIONS

Assume $p < \sqrt{D}/2$ is a rational prime that splits or ramifies into principal prime ideals in the ring extension $\mathbb{Z}[\sqrt{d}]/\mathbb{Z}$. Write $p\mathbb{Z}[\sqrt{d}] = P\bar{P}$. Let $\xi \in P$ and $\tilde{\xi} \in \bar{P}$ be the least elements of P, \bar{P} among those greater than 1. Then $\xi, \tilde{\xi} < \varepsilon_d$ and $\xi\tilde{\xi}$ is an irrational quadratic integer associated to p , which is necessarily $p\varepsilon_d$.

In the above literature, suppose d is sufficiently large and $p(p+1) < (1-\epsilon)\sqrt{d}$ (see the note below lemma 1.0.3). Since the periodic block of \sqrt{d} is symmetric and there are at most two total quotients that correspond to the same prime norm (see [16]), it follows that $\xi = \xi_m$ and $\tilde{\xi} = \xi_{l-m-2}$ for some $m < l$. It also worths noting that if ξ is ramified, then l is necessarily even and $\xi = \xi_{l/2-1}$. In particular, there can be only one such small ramified principal prime. Recalling the ramification criterion of 2, this proves the following; if $\epsilon > 0$ is fixed, for every sufficiently large square-free integer d congruent to 2 or 3 modulo 4 that is divisible by a prime less than $(1-\epsilon)d^{1/4}$, the class number h_d is greater than 1. Similar result obviously holds for $d \equiv 1 \pmod{4}$ with two or more prime divisors less than $(1-\epsilon) \left(\frac{1+\sqrt{d}}{2}\right)^{1/2}$. This is a weaker statement than what Gauss' genus theory tells us, namely, if t primes ramify in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ then $2^{t-1} | h_d^+$ (the order of the narrow class group) and hence $2^{t-2} | h_d$. This gives a demonstration of the connection between 'analytic' approach and 'algebraic' approach to the ideal class group.

Now recall theorem 4.0.9. It says that for any pair (y, x) with $0 \leq x < y$, $x^2 \equiv \pm 1 \pmod{y}$ there arises a quadratic sequence $\{d(n)\}_n$ where n runs through an arithmetic progression. In this section we replace the norm ± 1 by any integer μ and verify that for any pair (y, x) where x and y are relatively prime and $x^2 \equiv \mu \pmod{y}$, an arithmetic progression of n arises that gives rise to a quadratic sequence $\{d(n)\}_n$ such that $N(ny + x + y\sqrt{d})$ becomes μ , i.e., there exists a principal ideal of norm μ in the ring $\mathbb{Z}[\sqrt{d}]$.

Recall that for every d , any quadratic integer in $\mathbb{Z}[\sqrt{d}]$ with norm $\mu < \sqrt{d}$ comes from a convergent to \sqrt{d} (or is possibly a multiple of such quadratic integer, if μ has a square factor). If $n + x/y$ is a convergent to \sqrt{d} that gives norm μ , we have

$$N(ny + x + y\sqrt{d}) = n^2y^2 + 2nxy + x^2 - y^2d = \mu$$

and hence

$$x^2 \equiv \mu \pmod{y} \quad \text{and} \quad 2xyn \equiv -x^2 + \mu \pmod{y^2}.$$

Conversely, if $x^2 \equiv \mu \pmod{y}$ and $2xyn \equiv -x^2 + \mu \pmod{y^2}$, put

$$(5.0.1) \quad d = n^2 + \frac{2x}{y}n + \frac{x^2 - \mu}{y^2}$$

and it immediately follows that

$$N(ny + x + y\sqrt{d}) = \mu.$$

The condition $n^2 < d < (n+1)^2$ is equivalent to $2xyn - 2ny^2 - y^2 + x^2 < \mu < 2xyn + x^2$. If $0 \leq x < y$, it is equivalent to $n > \frac{\mu - x^2}{2xy}$. Observe that in a technical perspective, there is no necessity to confine the argument to n 's in this range.

Writing $2xyn \equiv -x^2 + \mu \pmod{y^2} \iff 2n \equiv \frac{-x^3 + \mu x}{y} \mu^{-1} \pmod{y}$, we proved the following theorem. Let

$$I(\mu) = \{(y, x) \in \mathbb{Z}^2 \mid 0 \leq x < y, \gcd(x, y) = 1, x^2 \equiv \mu \pmod{y}\}.$$

Theorem 5.0.13. *For every pair $(y, x) \in I(\mu)$, the set of n 's for which there exists an integer d such that $N(ny + x + y\sqrt{d}) = \mu$ forms an arithmetic progression with common difference \tilde{y} . In that case, the integer d is given by (5.0.1).*

Generalizing the notions of $\mathfrak{D}(y, x)$ and $\overline{\mathfrak{D}}(y, x)$, for each pair $(y, x) \in I(\mu)$ we define

$$\begin{aligned} \mathfrak{D}(\mu; y, x) &= \{d \in \mathbb{Z}_{>0} \mid \text{there exists } n \text{ s.t. } N(ny + x + y\sqrt{d}) = \mu\}, \\ \overline{\mathfrak{D}}(\mu; y, x) &= \{d \in \mathfrak{D}(\mu; y, x) \mid 1 < ny + x + y\sqrt{d} \leq \varepsilon_d\}, \\ \widehat{\mathfrak{D}}(\mu; y, x) &= \{d \in \overline{\mathfrak{D}}(\mu; y, x) \mid d \text{ is square-free}\}. \end{aligned}$$

Remark 5.0.14. If $n > \frac{\mu - x^2}{2xy}$ then $n^2 < d < (n+1)^2$, and when $d > \mu^2$, $n + x/y$ is a convergent to \sqrt{d} .

Remark 5.0.15. In case μ is a prime, say p , theorem 5.0.13 gives a list of d such that the prime ideals in $\mathbb{Q}(\sqrt{d})$ lying over p are principal. The union of $\widehat{\mathfrak{D}}(p; y, x)$ over all $(y, x) \in I(p)$ gives a complete list of real quadratic number fields in which p ramifies or splits into principal ideals, with possible

exceptions for $d \equiv 1 \pmod{4}$ which will be covered in section 6. The collection of sets $\{\widehat{\mathfrak{D}}(\mu; y, x)\}_{y,x}$, however, does not form a partition of these fields exactly. d is contained in a unique $\widehat{\mathfrak{D}}(p; y, x)$ only when p is ramified in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ into principal ideals; when p splits, there are two pairs (y, x) such that $d \in \widehat{\mathfrak{D}}(p; y, x)$.

Remark 5.0.16. Let d_0 be the least element of $\mathfrak{D}(p; y, x)$ and n_0 the associated integer that gives norm p in the above context. Let $d \in \mathfrak{D}(p; y, x)$. Since y and p are relatively prime, one can write

$$\begin{aligned} d = d(k) &= (n_0 + \tilde{y}k)^2 + \frac{2x}{y}(n_0 + \tilde{y}k) + \frac{x^2 - p}{y^2} \\ &\equiv (n_0 + \tilde{y}k)^2 + \frac{2x}{y}(n_0 + \tilde{y}k) + \frac{x^2}{y^2} \pmod{p} \\ &\equiv \left(n_0 + \tilde{y}k + \frac{x}{y}\right)^2 \pmod{p} \end{aligned}$$

so there exists a unique k modulo p that makes d divisible by p . For every pair $(y, x) \in I(p)$, therefore, the set of n 's that give the subset $\mathfrak{D}_{ram}(p; y, x)$ of $\mathfrak{D}(p; y, x)$ for which p ramifies forms an arithmetic progression with common difference $\tilde{y}p$. This can be a bit strange, because there is no way of *inertia* for the fields given by $\mathfrak{D}(p; y, x)$. When square-free integers are lined according to their size, an odd prime p ramifies and splits in $1/p$ and $\frac{p-1}{2p}$ of the corresponding fields respectively. Hence it may be natural to expect that about $\frac{2}{p-1+2}$ out of $\mathfrak{D}(p; y, x)$ will give fields in which p ramifies. The above equation shows, however, that this ratio is $1/p$.

Remark 5.0.17. When $d \in \mathfrak{D}_{ram}(p; y, x)$ and $d > p^2$, as mentioned before

$$\varepsilon_d = \frac{1}{p} \left(\lfloor \sqrt{d} \rfloor y + x + y\sqrt{d} \right)^2.$$

Note that if a real quadratic number field with large discriminant divisible by 4 has class number 1, its fundamental unit is of this form where we take $p = 2$.

The number of elements in $\mathfrak{D}(\mu; y, x)$ that are square-free has an asymptotic estimation. We state a lemma first.

Lemma 5.0.18. *Let p be an odd prime and $f(x) \in \mathbb{Z}[x]$ a quadratic polynomial whose leading coefficient is not divisible by p^m . Then $f(x) \equiv 0 \pmod{p^m}$ has a solution if and only if the discriminant of $f(x)$ is a square modulo p^m .*

Proof. (\Leftarrow) Clear.

(\Rightarrow) Let $t \in \mathbb{Z}$ be a solution to the modular equation. Then

$$f(t + pj) = f(t) + f'(t)pj + \frac{f''(t)}{2}p^2j^2.$$

Let $p^r \parallel f'(t)$. Choose α so that $f(t) + \alpha \equiv 0 \pmod{p^M}$ where M is sufficiently large. Note that α is necessarily divisible by p^m . We have

$$\begin{aligned} f(t + p^{r+1}j_1) + \alpha &= f(t) + \alpha + \frac{f'(t)}{p^r}p^{2r+1}j_1 + \frac{f''(t)}{2}p^{2r+2}j_1^2 \\ &\equiv f(t) + \alpha + \frac{f'(t)}{p^r}p^{2r+1}j_1 \pmod{p^{2r+2}}, \end{aligned}$$

$$\begin{aligned} f(t + p^{r+1}j_1 + p^{r+2}j_2) + \alpha &= f(t + p^{r+1}j_1) + \alpha + f'(t + p^{r+1}j_1)p^{r+2}j_2 \\ &\quad + \frac{f''(t + p^{r+1}j_1)}{2}p^{2r+4}j_2^2. \end{aligned}$$

Writing $f'(t + p^{r+1}j_1) = f'(t) + f''(t)p^{r+1}j_1$,

$$f(t + p^{r+1}j_1 + p^{r+2}j_2) + \alpha \equiv f(t + p^{r+1}j_1) + \alpha + \frac{f'(t)}{p^r}p^{2r+2}j_2 \pmod{p^{2r+3}},$$

and successively, there exists a unique sequence (j_1, j_2, j_3, \dots) such that $t + p^{r+1}j_1 + p^{r+2}j_2 + p^{r+3}j_3 + \dots \in \mathbb{Z}_p$ is a root of $f(x) + \alpha$. Since $\mathbb{Z}_p[x]$ is a UFD, it follows that the discriminant of $f(x) + \alpha$ is a square in \mathbb{Z}_p and hence that of $f(x)$ is a square modulo p^m . \square

Now we give the estimation.

Theorem 5.0.19. *Let $f(N)$ and $\widehat{f}(N)$ be the number of elements of $\mathfrak{D}(\mu; y, x)$ and $\widehat{\mathfrak{D}}(\mu; y, x)$ less than N . Then*

$$\lim_{N \rightarrow \infty} \frac{\widehat{f}(N)}{f(N)} = \left(1 - \frac{\omega_d(2)}{4}\right) \cdot \prod'_{p|y} \left(1 - \frac{1}{p^2}\right) \cdot \prod'_{p^2|\mu} \left(1 - \frac{1}{p}\right) \cdot \prod'_{p \nmid \mu y, \left(\frac{\mu}{p}\right)=1} \left(1 - \frac{2}{p^2}\right)$$

where the restricted products are over odd primes, and

$$\omega_d(2) = \begin{cases} 2 & \text{if } y \text{ is odd and } \mu \equiv 0 \text{ or } 1 \pmod{4}; \\ 2 & \text{if } 2|y, 4 \nmid y, \mu \equiv 1 \pmod{8}; \\ 1 & \text{if } 4|y; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $d_0 = d_0(\mu; y, x)$ be the least element of $\mathfrak{D}(\mu; y, x)$ and n_0 the associated integer that gives norm μ . By theorem 5.0.13, the elements of

$\mathfrak{D}(\mu; y, x)$ are given by a quadratic polynomial

$$\begin{aligned} d = d(k) &= (n_0 + k\tilde{y})^2 + 2\frac{x}{y}(n_0 + k\tilde{y}) + \frac{x^2 - \mu}{y^2} \\ &= \tilde{y}^2 k^2 + \left(\frac{2\tilde{y}}{y}x + 2\tilde{y}n_0 \right) k + d_0 \end{aligned}$$

for nonnegative integers k .

We use the notations of theorem 2.0.5. Let δ be the discriminant of the quadratic polynomial $d(k)$ and $\omega'_d(p)$ the number of solutions to $d(k) \equiv 0 \pmod{p^2}$ in the range $0 \leq k < p^2$. When y is even, $\delta = (x + yn_0)^2 - y^2 d_0 = \mu$ and similarly $\delta = 4\mu$ when y is odd. Therefore $d(k)$ has no repeated root. Note that $\omega'_d(p) < p^2$ implies $p \nmid B'$ and hence $q_p = 0$.

We consider odd primes first. Clearly $d(k) \pmod{p}$ is singular if and only if $p \mid \tilde{y}\mu$. For $p \nmid \tilde{y}\mu$, every root of $d(k) \equiv 0 \pmod{p}$ has a unique lifting to a p -adic root. There exists such a root if and only if the discriminant is a square modulo p , whence we have

$$w'_d(p) = \begin{cases} 2 & \text{if } \left(\frac{\mu}{p} \right) = 1; \\ 0 & \text{if } \left(\frac{\mu}{p} \right) = -1. \end{cases}$$

If $p \mid \tilde{y}$, $d(k)$ is congruent to $(x + yn_0)k + d_0$ or $2(x + yn_0)k + d_0$ modulo p^2 , which has a unique solution and hence $\omega'_d(p) = 1$.

When $p \mid \mu$, $d(k) \equiv 0 \pmod{p}$ has a double root. Let t be the root of this equation in the range $0 \leq t < p$. From $d(t + pj) \equiv d(t) + d'(t)pj \pmod{p^2}$ and $d'(t) \equiv 0 \pmod{p}$, it follows that $d(k) \equiv 0 \pmod{p^2}$ has p roots if $d(t) \equiv 0 \pmod{p^2}$ or none otherwise. By lemma 5.0.18, $d(k) \equiv 0 \pmod{p^2}$ has a root if and only if the discriminant μ (or 4μ) is a square modulo p^2 , which in this case is equivalent to $p^2 \mid \mu$. Thus $\omega'_d(p) = p$ if $p^2 \mid \mu$ and $\omega'_d(p) = 0$ if not.

Now let $p = 2$. Assume y is odd (so $2y \equiv 2 \pmod{4}$). Then

$$\begin{aligned} d(k) &\equiv k^2 + 2(x + yn_0)k + d_0 \\ &\equiv k^2 + 2(x + n_0)k + n_0^2 + 2xn_0 + x^2 - \mu \pmod{4} \end{aligned}$$

and

$$\begin{aligned} d(0) &\equiv d(2) \equiv n_0^2 + 2xn_0 + x^2 - \mu \pmod{4}, \\ d(1) &\equiv d(3) \equiv n_0^2 + 2xn_0 + x^2 - \mu + 1 + 2x + 2n_0 \pmod{4}. \end{aligned}$$

If n_0 is odd, $d(0) \equiv d(2) \equiv (x + 1)^2 - \mu \pmod{4}$ and $d(1) \equiv d(3) \equiv x^2 - \mu \pmod{4}$. If n_0 is even, $d(0) \equiv d(2) \equiv x^2 - \mu \pmod{4}$ and $d(1) \equiv d(3) \equiv$

$(x+1)^2 - \mu \pmod{4}$. It follows that $\omega'_d(2) = 2$ if $\mu \equiv 0, 1 \pmod{4}$ and $\omega'_d(2) = 0$ otherwise.

Now assume y is even (and x is necessarily odd). Suppose $y = 2\tilde{y}$ where \tilde{y} is odd. In a single line of computation we obtain

$$\begin{aligned} d(1) &\equiv d_0 + x + 3 \pmod{4}, \\ d(2) &\equiv d_0 + 2x \pmod{4}, \\ d(3) &\equiv d_0 + 3x + 3 \pmod{4} \end{aligned}$$

which shows that $\omega'_d(2) = 2$ when d_0 is even and $\omega'_d(2) = 0$ otherwise. Observe that

$$\mu = (x + yn_0)^2 - y^2d_0 \equiv 1 + 4n_0 + 4n_0^2 - 4d_0 \equiv 1 - 4d_0 \pmod{8}$$

and it follows that d_0 is even if and only if $\mu \equiv 1 \pmod{8}$.

Finally, suppose $4|y$. In this case $d(k) \equiv xk + d_0 \pmod{4}$, which has a unique solution to $d(k) \equiv 0 \pmod{4}$ and hence $\omega'_d(2) = 1$.

In every case $\omega'_d(p)$ is less than p^2 and $q_p = 0$. Applying theorem 2.0.5, the assertion follows. \square

6. THE SEQUENCES FOR $d \equiv 1 \pmod{4}$

Assume $d \equiv 1 \pmod{4}$ and let $\omega_d = \frac{1+\sqrt{d}}{2}$. It is possible for a field $\mathbb{Q}(\omega_d)$ to have every quadratic integer of norm p in $\mathbb{Z}[\omega_d] \setminus \mathbb{Z}[\sqrt{d}]$, so we cover such possible exceptions here. The content is exactly the same with only trifling changes in the equations.

The quadratic integers in $\mathbb{Z}[\omega_d]$ of norm $\mu < \omega_d - 1/2$ come from convergents to ω_d (or are multiples of such integers if μ has a square factor). If $\frac{ny+x+y}{y}$ is a convergent to ω_d that gives norm μ ,

$$N(ny + x + y\omega_d) = \left(ny + x + \frac{y}{2}\right)^2 - \frac{y^2}{4}d = \mu$$

or

$$((2n+1)y + 2x)^2 - y^2d = 4\mu.$$

In case y is even, $ny + x + y\omega_d \in \mathbb{Z}[\sqrt{d}]$ which is counted previously so we assume y is odd in this section. Then we have

$$x^2 \equiv \mu \pmod{y} \quad \text{and} \quad (2n+1)xy \equiv -x^2 + \mu \pmod{y^2}.$$

Conversely, if $x^2 \equiv \mu \pmod{y}$ and $(2n+1)xy \equiv -x^2 + \mu \pmod{y^2}$, put

$$(6.0.2) \quad d = (2n+1)^2 + \frac{4x}{y}(2n+1) + \frac{4x^2 - 4\mu}{y^2}$$

and it follows that

$$N(ny + x + y\omega_d) = \mu.$$

Observe that d is automatically congruent to 1 modulo 4.

Like before, there is no need to confine the above argument to convergents to ω_d if above congruences are satisfied. Writing $(2n+1)xy \equiv -x^2 + \mu \pmod{y^2} \iff n \equiv \left(\frac{-x^3 + \mu x}{y} \mu^{-1} - 1\right) 2^{-1} \pmod{y}$, we again proved the following theorem. Let

$$I^{\text{odd}}(\mu) = \{(y, x) \in I(\mu) \mid y \text{ is odd}\}.$$

Theorem 6.0.20. *For every pair $(y, x) \in I^{\text{odd}}(\mu)$, the set of n 's for which there exists an integer $d \equiv 1 \pmod{4}$ such that $N(ny + x + y\omega_d) = \mu$ forms an arithmetic progression with common difference y . In that case, the integer d is given by (6.0.2).*

As done previously, for each pair $(y, x) \in I^{\text{odd}}(\mu)$ define

$$\begin{aligned} \mathfrak{D}^1(\mu; y, x) &= \{d \in \mathbb{Z}_{>0} \mid \text{there exists } n \text{ s.t. } N(ny + x + y\omega_d) = \mu\}, \\ \overline{\mathfrak{D}}^1(\mu; y, x) &= \{d \in \mathfrak{D}(\mu; y, x) \mid 1 < ny + x + y\omega_d \leq \varepsilon_d\}, \\ \widehat{\mathfrak{D}}^1(\mu; y, x) &= \{d \in \overline{\mathfrak{D}}(\mu; y, x) \mid d \text{ is square-free}\}. \end{aligned}$$

Recall that μ and y are relatively prime. Let d_0 be the least element of $\mathfrak{D}^1(\mu; y, x)$ and n_0 the associated integer that gives norm μ . Then

$$\begin{aligned} d = d(k) &= (2(n_0 + yk) + 1)^2 + \frac{4x}{y}(2(n_0 + yk) + 1) + \frac{4x^2 - 4\mu}{y^2} \\ &\equiv (2(n_0 + yk) + 1)^2 + \frac{4x}{y}(2(n_0 + yk) + 1) + \frac{4x^2}{y^2} \pmod{4\mu} \\ &\equiv \left(2(n_0 + yk) + 1 + \frac{2x}{y}\right)^2 \pmod{4\mu}. \end{aligned}$$

Thus if μ is odd, there exists a unique k modulo μ that makes d divisible by μ . When μ is an odd prime, in particular, the remarks in section 5 carry over verbatim.

Theorem 5.0.19 also has its analogue. Let $(y, x) \in I^{\text{odd}}(\mu)$.

Theorem 6.0.21. *Let $f^1(N)$ and $\widehat{f}^1(N)$ be the number of elements of $\mathfrak{D}^1(\mu; y, x)$ and $\widehat{\mathfrak{D}}^1(\mu; y, x)$ less than N . Then*

$$\lim_{N \rightarrow \infty} \frac{\widehat{f}^1(N)}{f^1(N)} = \prod'_{p|y} \left(1 - \frac{1}{p^2}\right) \cdot \prod'_{p^2|\mu} \left(1 - \frac{1}{p}\right) \cdot \prod'_{p \nmid \mu y, \left(\frac{\mu}{p}\right)=1} \left(1 - \frac{2}{p^2}\right)$$

where the restricted products are over odd primes.

Proof. Write

$$\begin{aligned}
d = d(k) &= (2(n_0 + yk) + 1)^2 + \frac{4x}{y}(2(n_0 + yk) + 1) + \frac{4x^2 - 4\mu}{y^2} \\
&= 4(n_0^2 + 2yn_0k + y^2k^2) + 1 + 4n_0 + 4yk + \frac{4x}{y}(2n_0 + 1 + 2yk) \\
&\quad + \frac{4x^2 - 4\mu}{y^2} \\
&= 2y^2k^2 + 4(2yn_0 + y + 2x)k + d_0
\end{aligned}$$

The computations for odd primes are exactly the same as in the proof of theorem 5.0.19 except for some powers of 2 that appear as coefficients. As for $p = 2$, since d is always congruent to 1 modulo 4, $\omega'_d(2) = 0$. \square

7. HEURISTICS AND COMMENTS

We return to the ring $\mathbb{Z}[\sqrt{d}]$.

The Minimality. μ has to be a quadratic residue modulo y for every pair $(y, x) \in I(\mu)$, so y has no prime factor q such that $\left(\frac{\mu}{q}\right) = -1$. Unless $\mu = 1$, the sum $\sum \frac{1}{y^s}$ over all such y 's involves only a half of the primes in its Euler product form and its order is asymptotically $\asymp \zeta(s)^{1/2}$ as $s \rightarrow 1+$. Using the Chinese remainder theorem it is easy to see that the number of $x \in [0, y)$ satisfying $x^2 \equiv \mu \pmod{y}$ is a bounded multiple (that is, between a half and twice) of $2^{\omega(y)}$. Since $\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta(s)^2}{\zeta(2s)}$ (see theorem 301 of [13]), one sees that

$$\sum_{(y,x) \in I(\mu)} \frac{1}{y^s} \asymp \sum_{y : \mu \text{ is a square mod } y} \frac{2^{\omega(y)}}{y^s} \asymp \zeta(s) \text{ as } s \rightarrow 1+$$

Since we have an upper bound of the period of \sqrt{d} in terms of d (for example, proposition 3.0.7), we also have a lower bound of d_0 in terms of y, x which goes to the infinity as y grows. The sum $\sum_{(y,x) \in I(\mu)} \frac{1}{(y\sqrt{d_0(\mu; y, x)})^s}$ therefore becomes $o(\zeta(s))$ as $s \rightarrow 1+$. Recalling that almost all real quadratic integers greater than 1 with given norm are minimal (see [16]), the sum $\sum \frac{1}{\xi^s}$ over all minimal ξ 's with norm μ is asymptotically in the same order of $\sum_{n > \sqrt{\mu}} \frac{1}{(n + \sqrt{n^2 - \mu})^s} \asymp \zeta(s)$ as $s \rightarrow 1+$. In an expository manner, this means that when a number $\xi = n + \sqrt{n^2 - \mu}$ with norm μ is picked, it is almost always minimal in the quadratic field $K = \mathbb{Q}(\xi)$, but the square-free integer d in $K = \mathbb{Q}(\sqrt{d})$ is almost always not minimal for the associated pair (y, x) where $\xi = n_d y + x + y\sqrt{d}$ for some integer n_d .

The Density of Discriminants. It is very natural to ask the density of d 's for which p splits or ramifies into principal prime ideals, or equivalently d 's such that p is in the image of $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}$. This is in fact trivially zero because such d must not be divisible by any prime factor q with $\left(\frac{p}{q}\right) = -1$ and these 'special' integers constitute only a null set in \mathbb{Z} . More meaningful question is therefore to ask the portion of d 's that give principal primes over p out of all those special integers.

We consider a general integer μ that need not be a prime. The sum $\sum_{(y,x) \in I(\mu)} \frac{1}{y^s}$ is asymptotically $\asymp \zeta(s)^2$ if $\mu = 1$ and $\asymp \zeta(s)$ if $\mu \neq 1$ as mentioned above, and when $\mu \neq 1$ the constructions of $I(\mu)$ and $\widehat{\mathfrak{D}}(\mu; y, x)$ are pretty the same. So we can expect the density of

$$\bigcup_{(y,x) \in I(\mu)} \widehat{\mathfrak{D}}(\mu; y, x)$$

for $\mu \neq 1$ to be always comparable with

$$\bigcup_{(y,x) \in I(-1)} \widehat{\mathfrak{D}}(-1; y, x).$$

This counts the discriminants whose fundamental unit has norm -1 , which is possible only when every odd prime factor of d is congruent to 1 modulo 4. It is well known that the number of such special d 's less than N is of the order $\frac{N}{\sqrt{\log N}}$, and it is a recent result that a positive portion between 41% and 67% out of them satisfies $N(\varepsilon_d) = -1$ (see Theorem 1 of [9] and the comments below it). We may expect that similar results can be found for prime numbers instead of -1 too.

Linearity of Norms. Note that $N(ny + x + y\sqrt{d}) = (ny + x)^2 - y^2d$ is a linear function with respect to d . As noted in proposition 4.0.8, every fixed predecessor $n + \frac{x}{y} = [n, a_1, a_2, a_3, \dots, a_m]$ specifies an interval whose length is approximately $\frac{2n}{y^2}$ and in that interval the absolute value of norm ν_m changes linearly from 1 to $2n$. It is a simple observation on proposition 4.0.8 that for every index $m \geq 1$, $a_m = 1$ for a half of the integers, $a_m = 2$ for $\frac{1}{2 \cdot 3} = \frac{1}{6}$ of the integers, $a_m = 3$ for $\frac{1}{3 \cdot 4} = \frac{1}{12}$ of the integers and so on. It worths writing down this as a proposition.

Proposition 7.0.22. *Write $\sqrt{d} = [a_0, a_1, a_2, \dots]$ and $\frac{p_m}{q_m} = [a_0, a_1, \dots, a_m]$. For every $m \geq 0$ and $0 \leq a \leq b \leq 1$, the density of (non-square) integers d satisfying*

$$a < \left| \frac{N(p_m + q_m\sqrt{d})}{2\sqrt{d}} \right| < b$$

is $b - a$.

The density $b - a$ is still valid for a fixed (y, x) if the interval defined by the predecessor x/y is long enough. This is true when $y = o(d^{1/4})$, but the technical difficulty lies in the case $y \gg d^{1/4}$ which may lead to conjecture 1.0.1.

A Cubic Surface. Assume n is fixed instead of μ . Recall that a triple (μ, y, x) with $\mu < n$, $\gcd(x, y) = 1$ satisfying

$$(7.0.3) \quad x^2 \equiv \mu \pmod{y} \quad \text{and} \quad 2xyn \equiv -x^2 + \mu \pmod{y^2}$$

gives a non-square integer d between n^2 and $(n+1)^2$ such that $N(ny + x + y\sqrt{d}) = \mu$. This means that a quadratic integer of norm μ appears (as ξ_m for some m) in the continued fraction expansion of \sqrt{d} .

Consider μ as a variable that is between $-2n$ and $2n$ (we let μ vary in this range rather than $[-n, n]$ because the norms ν_m vary this much). Equation 7.0.3 can be easily reformulated to a cubic surface whose integer solutions (t, y, x, μ) are of interest, namely

$$(7.0.4) \quad ty^2 + 2\mu ny = x^3 + \mu x.$$

Let $f_n(M; Y)$ be the number of solutions (t, y, x, μ) to 7.0.4 with $\mu = M$, $0 < y < Y$. Since the number of reduced integral ideals of a given norm is bounded, broadly speaking the period $l(\sqrt{d})$ is long if and only if the convergents to \sqrt{d} give many values of ν_m . In terms of the cubic surface, this is equivalent to saying that $f_n(M; Y)$ is comparable with $f_n(1; Y)$ for many M 's in $-2n \leq M \leq 2n$ as $Y \rightarrow \infty$. (A numerical tendency of $f_n(M; Y)$ can be seen in the following list; $f_2(\pm 1; 10^{17}) = 82$, $f_2(\pm 2; 10^{17}) = 33$, $f_2(\pm 3; 10^{17}) = 29$, $f_2(\pm 4; 10^{17}) = 23$ and $f_3(\pm 1; 10^8) = 45$, $f_3(\pm 2; 10^8) = 13$, $f_3(\pm 3; 10^8) = 19$, $f_3(\pm 4; 10^8) = f_3(\pm 5; 10^8) = f_3(\pm 6; 10^8) = 11$).

REFERENCES

1. C.Friesen, *On continued fractions of given period*, Proc. Amer. Math. Soc (1988), no. 103, 9–14.
2. Jia Chao-Hua, *The distribution of square-free numbers*, Sci. China Ser. A (1993), 154–169.
3. C.Hooley, *On the power free values of polynomials*, Mathematika **14** (1967), 21–26.
4. ———, *A note on square-free numbers in arithmetic progressions*, Bull. London Math. Soc. **7** (1975), 133–138.
5. ———, *On the pellian equation and the class number of indefinite binary quadratic forms*, J. Reine Angew. Math. **353** (1984), no. 2, 98–131.
6. J. H. E. Cohn, *The length of the period of the simple continued fraction of $d^{1/2}$* , Pacific J. Math.
7. E.Fouvry and F.Jouve, *A positive density of fundamental discriminants with large regulator*, Preprint.

8. ———, *Size of regulators and consecutive square-free numbers*, Preprint.
9. E.Fouvry and J.Klüners, *On the negative pell equation*, Ann. of Math.(2) **172** (2010), no. 3, 2035–2104.
10. E.V.Podsypanin, *Length of the period of a quadratic irrational*, Studies in number theory. Part 5, Zap. Nauchn. Sem. LOMI, 82, "Nauka" (1979), 95–99, (in Russian).
11. F.Halter-Koch, *Continued fractions of given symmetric period*, Fibonacci Quart. (1991), no. 29, 298–303.
12. F.Kawamoto and K.Tomita, *Continued fractions and certain real quadratic fields of minimal type*, J. Math. Soc. Japan **60** (2008), no. 3, 865–903.
13. G.H.Hardy and E.M.Wright, *An introduction to the theory of numbers*, fifth ed., Clarendon Press. Oxford, 1979.
14. A. Granville, *Abc allows us to count squarefrees*, Int. Math. Res. Not. (1998), no. 19, 991–1009.
15. H.Cohen and H.W.Lenstra, *Heuristics on class groups of number fields*, h.jager ed., Lecture Notes in Math., vol. 1068, 1984.
16. JH.Park, *On the regulators of real quadratic number fields*, Preprint.
17. K.Prachar, *Über die kleinste quadratfreie zahl einer arithmetischen reihe*, Monatsh.Math. **62** (1958), 173–176.
18. K.S.Williams and N.Buck, *Comparison of the lengths of the continued fractions of \sqrt{D} and $\frac{1}{2}(1 + \sqrt{D})$* , Proc. Amer. Math. Soc. **120** (1994), no. 4.
19. M.Beceanu, *Period of the continued fraction of \sqrt{n}* , Preprint (2003).
20. M.J.Jacobson, *Experimental results on class groups of real quadratic fields (extended abstract)*, Proc. 1998 Algorithmic Number Theory Sympos. **1423**, 463–474.
21. P.Kaplan N.Ishii and K.S.Williams, *On eisenstein's problem*, Acta Arith. (1990).
22. S.R.Finch, *Class number theory*, (2005).
23. Y.Yamamoto, *Real quadratic number fields with large fundamental units*, Osaka J. Math. **8** (1971), 261–270.

DEPARTMENT OF MATHEMATICS (ROOM 117), POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY, SAN 31 HYOGA DONG, NAM-GU, POHANG 790-784, KOREA.
TEL. 82-10-3047-7793.

E-mail address: pkskng@postech.ac.kr